



Technology Coordinators Manual For Online Testing

(Including Instructions for Secure Browser Installation on
Chromebooks, iPads, Macs, and Windows)

Badger Exam 3-8:
A Smarter Balanced Assessment

Updated March 10, 2015



Technology Coordinators Manual

TABLE OF CONTENTS

Introduction.....	5
Section 1: Network and Internet Requirements.....	5
Common Network Performance Bottlenecks	5
Bandwidth	6
Determining Bandwidth Requirements.....	7
Total number of students simultaneously testing.....	7
Size of the test content	7
Secure Browser Installation	8
Wireless Networking.....	8
Wireless access points	8
Recommendations on the optimal number of student workstations per wireless connection:	8
School Capacity Calculator	9
System Check Tool	10
Network Diagnostic Tools	10
Microsoft Windows specific tools	10
Mac OS X specific tools	11
Multi-Platform tools	11
Network Configurations	11
Protocols.....	11
Multi-purpose Internet Mail Extensions (MIME) Types.....	12
Uniform Resource Locators (URLs)	12
Domain name resolutions.....	12
Email server	12
Firewall, content filter, and proxy servers	12
Quality of Service (QoS)/Traffic shaping	13
Section 2: Hardware Requirements.....	14
Technology Requirements	14
Other Hardware Recommendations.....	15
Monitor/Screen Displays.....	15
Note about brightness/contrast:.....	15

Technology Coordinators Manual

Printers	15
Keyboards	15
Headphones.....	15
Section 3: Secure Browser.....	17
Chromebook Installation.....	17
Managed Chromebook Installation Procedure.....	17
Non-managed Chromebook Installation Procedure.....	19
Closing the Chromebook Secure Browser	20
Windows Secure Browser	20
Installing Windows Secure Browser	20
Manually installing the .exe package via the User Interface.....	20
Installing the .msi package via a script (Only applies to System and Network Administrators with appropriate privileges).....	21
Manually uninstalling the previous Windows Secure Browser	22
Disabling Fast User Switching in Windows	22
Disabling Fast User Switching in Windows XP (with Service Pack 3)	22
Disabling Fast User Switching in Windows Vista or 7	22
Disabling Fast User Switching in Windows 8.0 and 8.1	23
Closing the Windows Secure Browser	24
Network Installation for Windows (Network Administrators).....	24
Installing the Secure Browser to a shared drive.....	24
Pushing the Secure Browser installation directory from the network to client computers.	25
Terminal Server/Thin Client Installation (Windows).....	25
NComputing Virtual Desktop Installation (Windows)	27
Installing Secure Browser for Mac OS X 10.6–10.10.....	28
Disabling Spaces in Mission Control on Mac 10.7–10.10 computers.....	30
Uninstalling the previous Mac OS X Secure Browser	30
Network Installation Information for Mac OS X (Network Administrators)	30
Closing the Mac Secure Browser	31
Assistive Technology, Badger 3-8, Secure Browser	31
iOS (iPad) Secure Browser	32
Downloading and Installing the iOS Secure Browser	32

Technology Coordinators Manual

Enabling Guided Access.....	33
Activating Guided Access Before a Test Session Begins	35
Deactivating Guided Access After a Test Session Ends.....	35
Closing the iPad Secure Browser (iOS 6.0–6.1).....	36
Closing the iPad Secure Browser (iOS 7.0–8.1.2)	36
Section 4: Braille Hardware and Software.....	37
Braille Hardware	37
Braille Software	37
Requirements for Test Administrator Computers.....	37
Requirements for Student Computers	37
Applying Settings for Contracted/Uncontracted Braille.....	38
Adjusting JAWS Voice Profile	39
Adjusting JAWS Speaking Rate	39
Adjusting JAWS Punctuation.....	39
Section 5: Text-to-Speech	40
Secure Browser	40
Voice packs on Chromebooks.....	40
Configuring Text-to-Speech Settings	40
Windows XP.....	40
Windows 7	42
Windows 8.1	43
Section 6: User Support.....	44
Section 7: Local Caching Software	45
Appendix A: IP Addresses and URLs for Badger Exam Systems.....	46
IP Addresses and URLs for Badger Exam Systems.....	46
Appendix B – School Technology Coordinator Checklist	47
Document Change History	48

Technology Coordinators Manual

Introduction

The goal of this manual is to inform Technology Coordinators with the information necessary to install and configure the test delivery software required to deliver the Badger Exam to students.

Section 1: Network and Internet Requirements

A stable, high-speed (wired or wireless) Internet connection is required for online testing. The response time for each assessment depends on the reliability and speed of your school's Internet connection.

If your Internet connection is not working or stops working, students will need to complete their tests at a later time or on another day. Should this occur, any answers the students have submitted will be saved. When the student returns, he/she will resume testing where they left off and be returned to the first unanswered item in the test.

For the online testing applications to work properly, you may need to verify your network settings. If you are not sure whether your network is properly configured or you have questions, contact your network administrator or technology specialist to find the right contact person in your area.

Network configuration settings should include the following:

- Content filters, firewalls and proxy servers should be configured to allow traffic on the protocols and to the servers listed in the Network Configurations section.
- Session timeouts on proxy servers and other devices should be set to values greater than the average scheduled testing time. This will help limit network interruptions during testing. For example, if testing sessions are scheduled for 60 minutes, consider session timeouts of 65–70 minutes.
- Data caching needs to be disabled.
- If your client network uses any device(s) that performs traffic shaping, packet prioritization, or Quality of Service, the URLs or IP addresses specified in Appendix A should be given a high priority to guarantee the highest level of performance.
- URLs and IP addresses list in Appendix A should be open or whitelisted.

Common Network Performance Bottlenecks

All network communications are accomplished using the IP protocol suite. The LAN (local area network) must be able to route IP traffic to and from the Internet. The Test Delivery Engine is delivered directly through the Internet. Students must access their tests using the appropriate Secure Browser. (See Section 3 for Secure Browser information.) For testing to take place, all workstations where tests will be administered must have reliable Internet connectivity.

Should your diagnostic tests determine that your systems have: unreliable Internet connectivity, low bandwidth, or a high number of simultaneous testers; a helpful tool that can be used to

Technology Coordinators Manual

reduce those bandwidth bottlenecks is the Local Caching Software. The benefits of using the LCS are:

- Reduce the reliance on external Internet bandwidth.
- Increase the number of test-takers you can support.
- Automatic caching (and purging) of test data.
- LCS Monitoring Tool.
- Easy installation and maintenance.

More information on LCS, including system requirements and installation procedures will be in Section 7 of this manual in mid-March.

In general, the performance of the Test Delivery Engine will depend on a number of factors, including bandwidth, total number of students simultaneously testing, size of test content, Secure Browser installation, proxy server (if used) and the wireless networking solution (if used).

Bandwidth

Bandwidth is the measure of the capacity of a network. Utilized bandwidth measures the amount of data traveling across the network at a given point in time. Bandwidth performance can be affected on either of the following networks: internal network (LAN) traffic and Internet traffic from the router. Regardless of hardware or network topology, the LAN should be analyzed to determine the potential for traffic bottlenecks.

The following table displays the estimated average bandwidth used by the Secure Browser for testing. (Note that there is a one-time exception to these averages; during initial Secure Browser startup, the load can be greater.)

Number of Students Testing Concurrently in School/Building	Average Estimated Bandwidth Consumed During Testing*
1	20K bytes/second
50	250–750K bytes/second (0.25–0.75M bytes/second)
100	500–1500K bytes/second (0.5–1.5M bytes/second)

* Bandwidth will vary during a student's testing experience, as some test pages contain low-bandwidth content, such as selected-response items, and other pages contain higher-bandwidth content, such as animations, audio clips, or American Sign Language videos. Consequently, the estimated average values in this column are based on computing averages from multiple tests and test subjects.

Technology Coordinators Manual

Determining Bandwidth Requirements

Schools need to factor the bandwidth requirements of each test along with all other non-test-related Internet traffic in order to determine how many concurrent test sessions the schools' Internet connections can support.

The test includes animations and interactive item types. These may increase the bandwidth required, but the bandwidth should not exceed the peak usage experienced when the test initially loads. We encourage you to run the diagnostics on your network to determine how many students at a time you can reasonably test. Refer to the Network Diagnostics Tools section for information about running diagnostics on your network.

For wired networks, internal bandwidth is typically not a problem, because new switches generally operate at speeds of between 100M bits per second and 1000M bits per second. However, LAN performance can be hindered in cases where hubs are used instead of switches. A hub device will allow broadcast signals from various network devices to propagate across the network, potentially saturating the network and causing traffic competition and/or collisions of data.

For Internet networks, the most common bottleneck is the ISP's router connection, which typically operates at speeds of between 1.5M bits per second and 100M bits per second. Network administrators should spend time prior to test administration determining whether their Internet infrastructure has the capacity to accommodate current and future growth.



Determining whether the infrastructure is capable of current and future growth involves a number of steps, including but not limited to:

- Analysis of the current number of users.
- Current day-to-day Internet bandwidth statistics.
- Desired response time for applications.

Total number of students simultaneously testing

As the number of students testing at one time increases, competition for network bandwidth increases. Network bandwidth resembles highway traffic; as the number of cars traveling on a given road increases, the speed of traffic flow decreases.

It is recommended that all schools use a Local Caching System (LCS). This will minimize the use of Internet bandwidth in schools to reduce the possibility for issues and maximize the number of students who can be tested simultaneously. For more using an LCS, see Section 7.

Size of the test content

The size of the test is determined by two factors: (1) the number of items on the test and (2) the average size of each item. The more items a test contains and the larger the average size of a test item, the higher the bandwidth requirement for a given test. For example, ELA tests

Technology Coordinators Manual

typically deliver all items associated with a passage at one time, and this may slightly increase the bandwidth for these tests.

Secure Browser Installation

The recommended installation of the Secure Browser(s) is local installation on each individual testing workstation. It is possible to install the Secure Browser on a network or shared drive and then have the testing workstations run the Secure Browser from that drive, but there may be some performance impacts under this configuration. There will be competition for network bandwidth and the network or shared disk drive will also be subject to some resource competition as there will be multiple clients reading from the network drive, thus slowing the overall processing speed.

Wireless Networking

Over the past several years, there have been several revisions to wireless networking technology.

- 802.11ac is the fastest and most recent IEEE wireless standard, with a throughput of up to 1.3G bits per second.
- 802.11n has a theoretical throughput of up to 300M bits per second.
- 802.11g has a theoretical throughput of up to 54M bits per second.
- 802.11b has a theoretical throughput of 11M bits per second.



Wireless Security – Due to the sensitivity of test-related data, encryption is required. It is highly recommended that wireless traffic use WPA2/AES data encryption. Because encryption/decryption is part of the data exchange process, there may be a slight decrease in the overall speed of the network.

Wireless access points

It is recommended that schools maintain a ratio of wireless systems to wireless access points (WAPs) of no more than 20 to 1. Typically, the test performance begins to deteriorate after that threshold has been reached. In some instances, older WAPs may also see performance degradation when more than 15 devices are concurrently attached.

Recommendations on the optimal number of student workstations per wireless connection:

The optimal (or maximum) number of student workstations (computers and tablets) supported by a single wireless connection will depend on the type of networking standard being used for the connection. The two most common networking standards are 802.11g (54Mbps) and the newer and faster standard, 802.11n (300Mbps). Both the access point, which emits the wireless signal, and the computer's wireless card, which receives the signal, will use one of these two standards. The recommendations below are based on the standard in use:

Technology Coordinators Manual

	802.11g Access Point	802.11n Access Point
802.11g Wireless Cards	20 workstations or devices	40 workstations or devices
802.11n Wireless Cards	20 workstations or devices	40 workstations or devices
Mix of 802.11g and 802.11n Wireless Cards	20 workstations or devices	40–50 workstations or devices (depending on the ratio of wireless cards used)



NOTE: Refer to your vendor's wireless access point documentation (e.g. user manual, white papers) for specific recommendations and guidelines.

School Capacity Calculator

The School Capacity Calculator at <http://oea.dpi.wi.gov/assessment/Smarter>. School Capacity Calculator can assist in planning for the test administration. The School Capacity Calculator can be used to find the maximum student capacity, the minimum required computers, the minimum test sessions per day, and the minimum required days of testing.

To determine the Maximum Student Capacity, enter the number of computers, the number of test sessions available per day, and the number of days allowed for testing. Select the "Calculate" button and the system will provide the maximum student capacity for testing.

To determine the Minimum Required Computers, enter the number of student administrations, the number of test sessions available per day, and the number of days allowed for testing. Select the "Calculate" button and the system will provide the minimum number of computers required for testing.

To determine the Minimum Test Sessions per Day, enter the number of computers, the number of student administrations, and the number of days allowed for testing. Select the "Calculate" button and the system will provide the minimum number of sessions needed each day for testing.

To determine the Minimum Required Days, enter the number of computers, the number of student administrations and the number of sessions available per day. Select the "Calculate" button and the system will provide the minimum number of days needed for testing.

System Check
Check your system to see its level of readiness for testing implementation. To determine your bandwidth, select a test from the drop-down list and enter the maximum number of students likely to test at one time, then click Run Test.

! Your Operating System: **Windows 7** Your Browser Version: **Chrome 41.0.2272.3**

System Requirements
Find the system requirements for your device by clicking on the link below.
[System Requirements](#)

System Check Test
To determine your bandwidth, select a test from the drop-down list and enter the maximum number of students likely to test at one time, then click Run Test.

Enter # simultaneous testers:

[RUN TEST](#)

School Capacity Calculator
Use this calculator tool to estimate a school or test center's capacity to conduct online testing. Choose the option you would like to calculate below.

Select Calculation Type
Maximum Student Capacity

of Computers
 # of Test Sessions Available per Day
 # of Days Allowed for Testing

[CALCULATE](#)

Technology Coordinators Manual

System Check Tool

The System Check Tool is available at <http://oea.dpi.wi.gov/assessment/Smarter>, and can be used to analyze your bandwidth and level of readiness for testing implementation. Users should run the System Check Test from each connection at different times, different days, and different times of day to assess the available bandwidth and network traffic. Your school's bandwidth will vary with usage and traffic levels. For example, the administrative office could be uploading payroll or a class could be making use of videos.

System Check

Check your system to see its level of readiness for testing implementation. To determine your bandwidth, select a test from the drop-down list and enter the maximum number of students likely to test at one time, then click Run Test.

Your Operating System: Windows 7 **Your Browser Version: Chrome 41.0.2272.3**

System Requirements

Find the system requirements for your device by clicking on the link below.

[System Requirements](#)

System Check Test

To determine your bandwidth, select a test from the drop-down list and enter the maximum number of students likely to test at one time, then click Run Test.

Enter # simultaneous testers: [RUN TEST](#)

School Capacity Calculator

Use this calculator tool to estimate a school or test center's capacity to conduct online testing. Choose the option you would like to calculate below.

Select Calculation Type
Maximum Student Capacity

of Computers

of Test Sessions Available per Day

of Days Allowed for Testing

[CALCULATE](#)

Network Diagnostic Tools

If further diagnostic is needed the following is a list of system specific tools that can help identify your network bottlenecks and problems.

Microsoft Windows specific tools

PRTG Traffic Grapher (www.paessler.com/prtg)

This Windows software monitors bandwidth usage and other network parameters via Simple Network Management Protocol (SNMP). It also contains a built-in packet sniffer. A freeware version is available.

NTttcp (www.microsoft.com/whdc/device/network/TCP_tool.msp)

NTttcp is a multithreaded, asynchronous application that sends and receives data between two or more endpoints and reports the network performance for the duration of the transfer.

Pathping

Pathping is a network utility included in the Windows operating system. It combines the functionality of Ping with that of Traceroute (Windows filename: tracert) by providing details

Technology Coordinators Manual

of the path between two hosts and Ping-like statistics for each node in the path based on samples taken over a time period.

Mac OS X specific tools

Network Utility.app

This tool is built into Mac OS X software.

Multi-Platform tools

Wireshark (www.wireshark.org)

Wireshark (formerly Ethereal) is a network protocol analyzer. It has a large feature set and runs on most computing platforms including Windows, OS X, Linux, and UNIX.

TCPDump (<http://sourceforge.net/projects/tcpdump>)

TCPdump is a common packet sniffer that runs under the command line and is compatible with most major operating systems (UNIX, Linux, and Mac OS X). It allows the user to intercept and display data packets being transmitted or received over a network.

A Windows port WinDump is also available (www.winpcap.org/windump/).

Ping, NSLookup, Netstat, and Traceroute (in Windows: tracert)

This is a set of standard UNIX network utilities. Versions of these utilities are included in all major operating systems (UNIX, Linux, Windows, and Mac OS X).

Iperf (<http://sourceforge.net/projects/iperf/>)

Iperf measures maximum TCP bandwidth, allowing the tuning of various parameters and User Datagram Protocol (UDP) characteristics. Iperf reports bandwidth, delay jitter and datagram loss.

Network Configurations

Networks will need to be configured to allow for the protocols, MIME type, and URLs listed below.

Protocols

All communication with the network takes place over the following Internet port/protocol combinations. Please ensure that the following ports are open for these systems.

Port/Protocol	Purpose
80/tcp	HTTP (initial connection only)
443/tcp	HTTPS (secure connection)

Technology Coordinators Manual

Multi-purpose Internet Mail Extensions (MIME) Types

Allow downloading and uploading of these MIME types:

- application/json
- application/octet-stream
- image/png
- multipart/form-data
- printer/prn
- text/html
- text/xml
- video/mp4

Uniform Resource Locators (URLs)

Allow the URLs listed below to be accessed through the firewall:

- http://*.caltesting.org
- https://*.caltesting.org



NOTE: If white listing wildcard entries are not permitted, a full list of fully qualified domain names (FQDNs) and IPs can be found in Appendix A.

Domain name resolutions

All system URLs must be resolvable by all client hosts attempting to connect to the Test Delivery System. This means that the client workstations should be able to convert the friendly names (URLs) to their corresponding IP address by requesting the information from the DNS server.

Email server

Schools will need to make sure following email addresses are whitelisted to ensure delivery:

*@ets.org

*@caltesting.org

Firewall, content filter, and proxy servers

Content filters, firewalls, and proxy servers should be configured to allow traffic on the protocols listed above to the applications' servers. In addition, session timeouts on proxy servers and other devices should be set to values greater than the average duration it takes a student to complete a given test. For additional information and support, contact the Badger Exam Help Desk at 1-844-711-6493, or via email at badgerexamhelpdesk@ets.org.

Technology Coordinators Manual

Schools will need to make sure that information is not blocked in their content filters and that data are not cached. Please ensure that the IP addresses listed in Appendix A are open for these systems.

Quality of Service (QoS)/Traffic shaping

If the client network utilizes any device(s) that performs traffic shaping, packet prioritization, or Quality of Service, the URLs or IP addresses in Appendix A should be given a high level of priority in order to guarantee the highest level of performance.

Technology Coordinators Manual

Section 2: Hardware Requirements

Technology Requirements

The information in this section provides information regarding supported operating systems and related hardware recommendations as well as requirements for monitors/screens, printers, keyboards, and headphones.

Table 5 organizes requirements and recommended specifications for each supported operating system for desktops and laptops. Table 6 provides information regarding supported tablets.

Table 5. Requirements for Desktops and Laptops

Supported Operating Systems	Minimum Requirements for Current Computers	Recommended Minimum for New Purchases
Windows laptops and desktops Running Windows XP (service Pack 3), Vista, 7, 8.0, 8.1 Server 2003 and 2008 <i>Windows Surface is unsupported.</i>	Pentium 4 Processor and above 512 MB RAM 200 MB hard drive free space	1 GHz processor 1 GB RAM 80 GB hard drive
Mac OS X laptops and desktops Running OS X 10.6 to 10.10 <i>Mac OS 10.5 (Power PC and Intel) is unsupported.</i>	Intel x86 Processor 512 MB RAM 200 MB hard drive free space	

NComputing and Terminal Services are supported on the following platforms:

- NComputing is supported on computers running Windows XP (Service Pack 3) and Windows 7
- Terminal Services is supported on the Windows 2003, 2008 and 2012 servers

Table 6. Supported Mobile Operating Systems and Browsers Operating System Supported Devices

Device and Operating Systems	Minimum Requirements
iPad 2 and above Running iOS 6.0 to 8.1.3* <i>iPad mini is unsupported.</i>	Physical keyboard required
Chromebook Running Chrome v40 and 41 only* <i>Please disable any "automatic updates" to maintain v. 40 or v. 41</i>	2 GB RAM

*It is highly recommended that automatic updates of the iOS and Chrome operating systems be turned off or delayed. Doing so will allow changes to these systems to be reviewed and any that pose a potential risk to student testing to be addressed.

Note: The Linux and Android platforms are unsupported for the 2014-2015 school year.

Technology Coordinators Manual

Other Hardware Recommendations

The following information is general. Because of the myriad ways school networks and computers can be set up, we encourage you to verify diagnostics, especially with monitor resolution, and headphones.

Monitor/Screen Displays

Screen Dimensions: 10" class or larger; iPads with a 9.5" display are an accepted part of this class

Resolution: 1024 x 768 or better

Depending on the screen size, some individuals may need to use vertical and/or horizontal scroll bars to view all test-related information. Students may also use the Zoom tool in the online test to enlarge the content on the screen.

Note about brightness/contrast:

Some test items include images that are shaded. Because monitors and screens vary widely, we cannot guarantee that the "default" settings that monitors are shipped with are optimal. Monitor settings may need to be adjusted if a student says test items with shaded images (e.g., pie charts) are very light or cannot be seen.

Printers

We strongly suggest that Test Administrators be connected to a single local or network printer in the testing room. Only the Test Administrator's computer should have access to this printer to monitor any Print On Demand requests.

Keyboards

Students may use mechanical, manual, and Bluetooth-based keyboards. Some external keyboards have additional "shortcut" buttons that can create security issues. These buttons may allow students to open another application or the tablet's default on-screen keyboard.

When using wireless keyboards, ensure that there is sufficient physical space between students.

Headphones

All students will need headphones for the English language arts tests. The ELA tests contain items that have recorded audio.

Additionally, students needing the text-to-speech or audio glossaries on the mathematics tests will require headphones. Students using the Braille accommodation can use the Job Access with Speech (JAWS®) screen reading software to listen to mathematics assessments.

Technology Coordinators Manual

We encourage you to work with your School Test Coordinator to ensure that you have an adequate supply of headphones on hand.

USB headphones are recommended, as they are typically plug-and-play devices.

Refer to Section 5 for more information about Text-to-Speech and Voice.

Other Hardware Requirements for Badger Exam	
Additional Hardware	Minimum Requirement
Screen Size	Display must measure a minimum of 9.5 inches diagonal (sometimes described as “10-inch class”). Resolution must meet be a minimum of 1024x768.
Headphones/earphones	Headphones or earphones must be available to students for use during the English language arts test and for students who require text-to-speech features on the mathematics test. *Provided by student, school, or district.
Keyboards	A physical keyboard is required to avoid consuming screen space that must be available for test content.
Pointing Device	A pointing device must be included. This may be a mouse, touch screen, touchpad, or other pointing device with which the student is familiar.
Network	Must be connected to the internet with a minimum of 20KBps available per student to be tested simultaneously. For more details about Network Requirements, please see the Section 1 “Network and Internet Requirements”
Security	It must be possible to secure the device so that the student does not have access to unauthorized web sites or applications. This is accomplished through the use of the Secure Browser.

Technology Coordinators Manual

Section 3: Secure Browser

All students must use a Secure Browser to access the Badger Exam. The Secure Browser prevents students from accessing other computer or Internet applications or copying test information. All computers that will be used for testing must have the correct Secure Browser installed.

Below are the instructions for installing the Secure Browser for students that do not require assistive technology. Assistive Technology Secure Browser installation can be found on page 31 of this manual.

Before any installation occurs, be sure you have admin rights to the computer/device.

Chromebook Installation

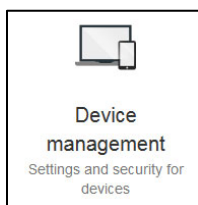
The following instructions cover the process of preparing and installing the Secure Browser on Chromebooks. Chromebooks are either managed centrally through the Google admin portal (aka Managed Chromebook), or managed individually on each device (aka Non-managed Chromebook). Determine how your Chromebooks are managed at your school and then select the appropriate starting procedure.



NOTE: Managed Chromebooks offer a centralized management, making software deployment consistent and highly efficient.

Managed Chromebook Installation Procedure

1. Set up your free Google Apps for Education account and enroll all managed Chromebooks.
See <http://www.google.com/intl/en/chrome/education/devices/features-management-console.html> for information.
2. Open a browser and navigate to <https://admin.google.com>.
3. Log in using your Google Apps for Education account.
4. Select Device Management.



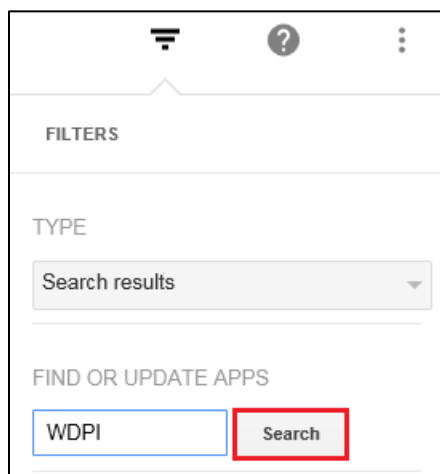
5. Select **Chrome** from the list of PLATFORMS.




6. Under Chrome Management, select **App Management**.

Technology Coordinators Manual

7. In the right-hand column, search for **WDPI** in “FIND OR UPDATE APPS” field <Search>.



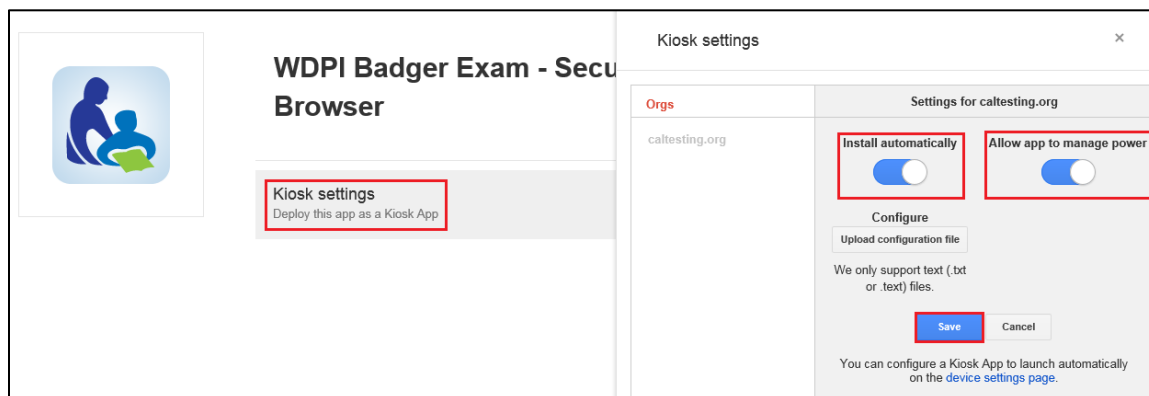
8. Click on the app title “WDPI Badger Exam – Secure Browser”.

←	Device management	>	Chrome	>	Chrome App Management
<input type="checkbox"/>	APPS				STATUS
<input type="checkbox"/>					WDPI Badger Exam - Secure Browser
					Not Configured

9. On the following screen, click on “**Kiosk Settings** Deploy this app as a Kiosk App”.

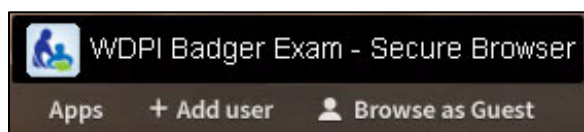
10. Select your organization (e.g. “caltesting.org”).

11. Enable “Install automatically”, “Allow app to manage power” and <Save>.



NOTE: The WDPI Badger Exam Secure Browser will appear on all managed Chromebooks. This may take up to 15 minutes.

12. To launch the Secure Browser, click the Apps link in the menu row of a managed Chromebook and select the WDPI Badger Exam - Secure Browser app.



Technology Coordinators Manual

Non-managed Chromebook Installation Procedure

1. Log in with staff/admin Google user account.



NOTE: Must log in with the Chromebook owner account.

2. Open a Chrome web browser and go to <chrome://extensions>.
3. Scroll to the bottom of the page, and click on **Get more extensions**.
This will open the Chrome Web Store in a new tab.
4. Type **WDPI** in the search field and press **Enter**.

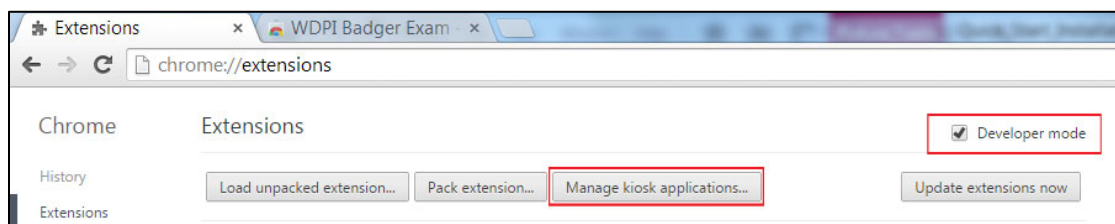
5. Click on the **WDPI Badger Exam – Secure Browser**.



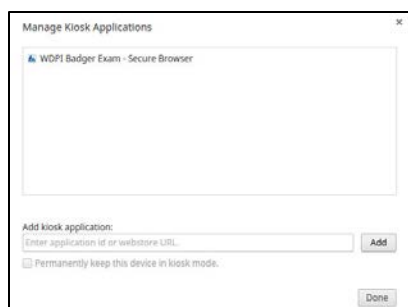
NOTE: Do NOT click on the **FREE** button to install.

The WDPI Badger Exam – Secure Browser will popup.

6. Click in the address bar (this will highlight the entire URL.)
7. Copy the URL to the clipboard with shortcut keys: Ctrl + C.
8. To return, click on the Extensions tab.
9. Scroll to the top of the page.
10. Verify the Developer Mode box (at the top of the page) is checked.
11. Click **Manage Kiosk Applications**. The Manage Kiosk Applications box will pop-up.

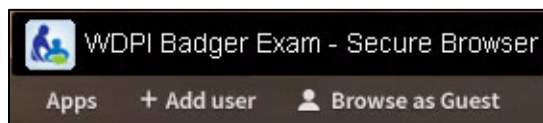


12. Click in the **Add kiosk applications:** field.
13. Paste the URL from the clipboard with shortcut keys: Ctrl + V.
14. Click **Add**, WDPI Badger Exam – Secure Browser will show up in the Manage Kiosk Application list.
15. Click **Done** and close the browser.



Technology Coordinators Manual

16. Sign out of the Chromebook.
17. To launch the Secure Browser, click the Apps link, and select the **WDPI Badger Exam - Secure Browser** app.



Closing the Chromebook Secure Browser

In the event that there is a need to force an exit of the Secure Browser before completion of a test, enter **Shift + Esc + E**.

Windows Secure Browser

This section provides instructions for installing the Windows Secure Browser on computers with Windows XP (Service Pack 3), Vista, 7, 8.0, or 8.1. Other Windows operating systems are not supported.

Installing Windows Secure Browser



IMPORTANT: All Windows installations will require Read/Execute permissions to the program folder, and Read/Write permissions to the user's home directory

Manually installing the .exe package via the User Interface

The following instructions cover the process of preparing and installing the Secure Browser on Windows devices.

1. Open a browser and go to the DPI Badger Portal at: <https://wdpibadger.caltesting.org> and click **DOWNLOADS**.
2. Select the **WDPI Badger Exam Secure Browser Windows EXE** button.



NOTE: For a network installation, select the **WDPI Badger Exam Secure Browser Windows MSI** button from the list of download options.

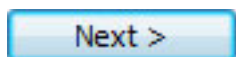


3. Select the securebrowser icon located on the desktop or downloads folder, or select "Run..." when the popup appears.

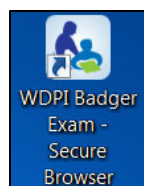


Technology Coordinators Manual

4. Follow the on screen installation directions to allow the software to install.



5. When the installation completes, the Secure Browser can be launched by double-clicking the Secure Browser icon on your desktop or go to:
Start Menu → All Programs → **WDPI Badger Exam - Secure Browser**



Installing the .msi package via a script (Only applies to System and Network Administrators with appropriate privileges)

Network administrators can install the Windows Secure Browser via an installation script to be executed by an Admin account in the machine. The script can be written to run without any human interaction (quiet switch) and to install in the default directory (C:\Program Files) or any target directory of choice. Un-installation can also be scripted.

Below are two generic scripts: one for installation and one for uninstallation. Both require the script to have visibility to the .msi installation file and can only be executed by an admin account on the machine. (This is a Windows-based restriction, not a Secure Browser restriction, as the msixec service that installs .msi files is meant to be used by administrators only.)

Script Conventions:

<Source> = Complete path to the Secure Browser msi installation file including .msi installation file name

Example: C:\MSI\securebrowser.msi

<Target> = Complete path to the location where the Secure Browser should be installed if the default location (C:\Program Files) is not preferred.

Example: C:\MSI\Installation_Dir



NOTE: The target install directory does not have to be created in advance.

1. Installation script: msixec /I <Source>/quiet INSTALLDIR=<Target> Example:
msixec /I C:\MSI\securebrowser.msi /quiet INSTALLDIR=C:\MSI\Browser_Install
2. Uninstallation script: msixec /X <Source>/quiet Example: msixec /X
C:\MSI\securebrowser.msi /quiet

Technology Coordinators Manual

Manually uninstalling the previous Windows Secure Browser

If you need to uninstall the previous Secure Browser for any reason, follow the steps below.

1. Open the Control Panel (from your taskbar, select Start > Settings > Control Panel).
2. Select Add or Remove Programs.
3. Select WDPI Badger Exam – Secure Browser and click [Remove] to open the Uninstall Wizard. Click [Next].
4. Click [Yes].
5. Click [OK] to complete the uninstall process.

Disabling Fast User Switching in Windows

Microsoft Windows (XP with Service Pack 3, Vista, 7, 8.0, and 8.1) allows computers to be configured so that multiple users can log into a computer without requiring one user to log out before another logs in.

This feature is called “fast user switching.”

If a student can access multiple user accounts from a single computer, disabling the Fast User Switching function is strongly encouraged. Instructions for doing so follow.

Disabling Fast User Switching in Windows XP (with Service Pack 3)

1. Click [Start], click [Control Panel], and then click [User Accounts].
2. Click [Change the Way Users Log On or Off].
 - a. Ensure the Use the Welcome Screen option is checked.
 - b. Ensure the Use Fast User Switching option is not checked.
3. Click [Apply Options].



NOTE: Fast User Switching is not an option if joined to a domain.

Disabling Fast User Switching in Windows Vista or 7

Method A: Access the Group Policy Editor

1. Click [Start], type gpedit.msc in the Start Search dialog box, and then press [Enter].
2. Navigate to the following location:
Local Computer Policy → Computer Configuration → Administrative Templates → System → Logon
3. Set Hide entry points for Fast User Switching to Enabled.

Technology Coordinators Manual

4. Close the Fast User Switching properties window.
5. Close the Group Policy window.



NOTE: Because the Group Policy Editor does not exist in certain editions of Windows Vista, you may need to configure these settings via the registry if this method is unavailable. See Method B for registry instructions.

Method B: Access the Registry

1. Click [Start], type regedit.exe in the Start Search dialog box, and press [Enter].
2. Navigate to the following location: HKEY_LOCAL_MACHINE → SOFTWARE → Microsoft → Windows → CurrentVersion → Policies → System
3. Right-click the System folder in the left pane.
4. Click New, [DWORD (32-bit) value].
5. Type in HideFastUserSwitching and press [Enter].
 - a. Click the HideFastUserSwitching value.
 - b. Type 1 into the Value data field and click [OK].
 - c. Close the Registry Editor window.

Disabling Fast User Switching in Windows 8.0 and 8.1

1. Navigate to the Search option (from the home screen, mouse to the lower right corner and then click the Search icon).
2. In the search box, type gpedit.msc. Double-click the gpedit icon in the Apps pane. The Local Group Policy Editor window will open.
3. Navigate to the following location: Computer Configuration → Administrative Templates → System → Logon
4. In the Setting pane, double-click “Hide entry points for Fast User Switching.”
5. Select “Enabled” and then click [OK].
6. Navigate to the Search option (from the home screen, mouse to the lower right corner and then click the Search icon).
7. In the search box, type run. The Run dialogue box will open.
8. Enter the command gpupdate /force into the text box and then click [OK]. (Note the space before the backslash.)
9. The Windows system command box will open. When you see the message “Computer Policy update has completed successfully,” then Fast User Switching has been successfully disabled.

Technology Coordinators Manual

Closing the Windows Secure Browser

In the event that there is a need to force an exit of the Secure Browser before completion of a test, enter **Shift + Esc + E**.

Network Installation for Windows (Network Administrators)

You can install the Secure Browser to all computers on a network by copying browser files from the network to individual computers or through third-party programs to run the installers, such as Apple Remote Desktop.

This section contains information for installing the Secure Browser via a network. Please follow the appropriate instructions for your network setup.

Installing the Secure Browser to a shared drive.

1. Install the browser onto your server, following the standard directions available in this document.
2. Map the network directory to where you installed the Secure Browser (in Step 1) on each client machine.
3. In the network location where you installed the Secure Browser, create a shortcut by right-clicking the WDPI Badger Exam - Secure Browser icon and selecting "Create Shortcut."
4. Optional: You may want to rename the new shortcut; e.g., WDPI Badger Exam - Secure Browser. (This becomes your shortcut link name that you will use in Step 3.)
5. In the properties of the shortcut, change the path to use the mapped path as if on the client machine.
6. To each user (computer) profile, add the following command, which will execute upon login through the user group login script:
7. COPY "<X> \WDPI Badger Exam - Secure Browser.lnk" "%USERPROFILE%\Desktop"



NOTE: <X> refers to the shared directory from which the browser will be run. The script will need to reference the correct directory.

Technology Coordinators Manual

Pushing the Secure Browser installation directory from the network to client computers.

1. Install the browser onto your server, following the standard directions available in this document.
2. Identify the network directory to which you saved the browser file. These instructions will refer to that network directory as <X>.
3. Identify the *target* directory on the local user computers that you will copy the browser file to. These instructions will refer to that directory as <Y>. Make sure that you have *write* access to <Y> on the local computers.



NOTE: Restricted users will have access only to certain folders on the local computers.

4. Create a shortcut in the network directory by right-clicking the securebrowser.exe icon and selecting "Create Shortcut." Rename the new shortcut, e.g., "WDPI Badger Exam - Secure Browser"



NOTE: In the shortcut Properties, the "Target" and "Start In" attributes will show the <X> network installation directory.

5. Change the shortcut properties ("Target" and "Start In" attributes) to the local computers' <Y> directory instead of the default <X> network directory. That way the Secure Browser shortcut will now point to the designated installation directory.
6. Add the following lines to the login script for each user, replacing your actual local and source network directories for <Y> and <X>.

```
IF EXIST <Y> GOTO DONE
XCOPY "<X>" "<Y>" /E /I
COPY "<Y>\WDPI Badger Exam - Secure Browser.lnk"
"%USERPROFILE%\Desktop"
:DONE
EXIT
```

Terminal Server/Thin Client Installation (Windows)

The following steps should be taken when computers on a Terminal Services network setup have a shared or generic login account and multiple users need to use that same account when logging into Terminal Services.

1. Create a batch file that runs the logon script for the Secure Browser.

This creates a unique profile folder in "Application Data" with a unique session name. This can be placed in the "Startup" folder on the "Start" menu (Start → Programs → Startup).

- a. As the Administrator, open Notepad.
- b. Copy and paste the below line into the Notepad file:

Technology Coordinators Manual

```
"C:\Program Files\WDPI Badger Exam - Secure Browser\WDPI  
Badger Exam - Secure Browser.exe" -CreateProfile  
%SESSIONNAME%
```

- c. Save the file as a batch file to the desktop (you may call it anything; e.g., logon.bat).
- d. Go to "User Configuration," which is in the Group Policy.

Start Menu → Run → type GPEdit.msc → Click [OK]

- e. Navigate to 'User Configuration' and expand the 'Windows Settings' folder.
 - f. Click "Scripts (Logon/Logoff)."
 - g. Select "Logon" and go to "Properties" (either by clicking the Properties link on the left and right-clicking "Logon" or selecting "Properties").
 - h. In the "Logon Properties" window, click the [Add] button.
 - i. Browse for the "Logon" batch file that you created in Step B.
 - j. Click the [OK] button to add the file.
 - k. Click the [APPLY] button and then close the "Logon Properties" window.
 - l. Close the "Group Policy" window.
2. Create a shortcut on the desktop of each client machine.



This will create shortcuts for the Secure Browser on the client machines.

- a. On the Terminal Server machine, locate the Secure Browser folder.
C:\Program Files\<SecureBrowserName> folder\
- b. Right-click the WDPI Badger Exam - Secure Browser.exe file and select "Send to → Desktop (Create Shortcut)."
- c. Right-click the shortcut icon on the desktop and select "Properties."
- d. In the 'Target' text box, type in the below line as shown:
32-bit Windows:

```
"C:\Program Files\WDPI Badger Exam - Secure Browser\WDPI  
Badger Exam - Secure Browser.exe" -CreateProfile  
%SESSIONNAME%
```

64-bit Windows:

```
"C: \Program Files(X86)\WDPI Badger Exam - Secure Browser\  
WDPI Badger Exam - Secure Browser.exe" -CreateProfile  
%SESSIONNAME%
```
- e. Click [OK] to close the Properties window.

(Optional: If you would like to rename the shortcut on the desktop, select the shortcut, press F2, and rename it from "kiosk.exe" to "WDPI Badger Exam - Secure Browser")

NComputing Virtual Desktop Installation (Windows)

The following steps should be taken to install the Secure Browser on a network that uses NComputing virtual desktops.

1. Create a batch file that runs the logon script for the Secure Browser.

This creates a unique profile folder in “Application Data” with a unique session name. This can be placed in the “Startup” folder on the “Start” menu (Start → Programs → Startup).

- a. As the Administrator, open Notepad.
- b. Copy and paste the below line into the Notepad file:
`"C:\Program Files\WDPI Badger Exam - Secure Browser\dBT\dBT.exe" -CreateProfile %SESSIONNAME%`
- c. Save the file as a batch file to the desktop (you may call it anything; e.g., logon.bat).
- d. Go to “User Configuration,” which is in the “Remote Administration Console” window.

Start Menu → All Programs → NComputing vSpace → vSpace Console → Expand “Local Computer Policy”

- e. Expand “User Configuration” and expand the “Windows Settings” folder.
- f. Click “Scripts (Logon/Logoff)”.
- g. Select “Logon” and go to “Properties” (either by clicking the Properties link on the left or right-clicking “Logon” and selecting “Properties”).
- h. In the “Logon Properties” window, click the [Add] button.
- i. Browse for the “Logon” batch file that you created in Step B.
- j. Click the [OK] button to add the file.
- k. Click the [APPLY] button and then close the “Logon Properties” window.
- l. Close the “Remote Administration Console” window.

2. Create a shortcut on the desktop of each client machine.



NOTE: This will create shortcuts for the Secure Browser on the client machines.

- a. On the Terminal Server machine, locate the Secure Browser folder.
C:\Program Files\<SecureBrowserName> folder\
- b. Right-click the WDPI Badger Exam - Secure Browser.exe file and select “Send To → Desktop (Create Shortcut)”
- c. Right-click the shortcut icon on the desktop and select “Properties”
- d. In the “Target” text box, type or copy/paste the below line as shown:
32-bit Windows:

```
"C:\Program Files\WDPI Badger Exam - Secure  
Browser\dBT\dBT.exe" -CreateProfile %SESSIONNAME%
```

64-bit Windows:

```
"C:\Program Files(X86)\WDPI Badger Exam - Secure Browser\  
WDPI Badger Exam - Secure Browser.exe" -CreateProfile  
%SESSIONNAME%
```

- e. Click [OK] to close the Properties window.

(Optional: If you would like to rename the shortcut on the desktop, select the shortcut, press F2, and rename it from "WDPI Badger Exam - Secure Browser.exe" to "WDPI Badger Exam - Secure Browser")

3. Login as an admin and run the application once.

Simply launching the Secure Browser and going to the diagnostics page is sufficient (you do not need to start a test). Note: In order to launch the Secure Browser on the client machines, users will need to double-click the shortcut created on the desktop.

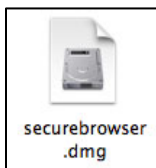
Installing Secure Browser for Mac OS X 10.6–10.10.

The following instructions cover the process of preparing and installing the Secure Browser on Mac OS X 10.6-10.10 devices.

1. Open a browser and go to the DPI Badger Portal at: <https://wdpibadger.caltesting.org> and click **DOWNLOADS**.
2. Select the **WDPI Badger Exam Secure Browser MAC DMG** button.



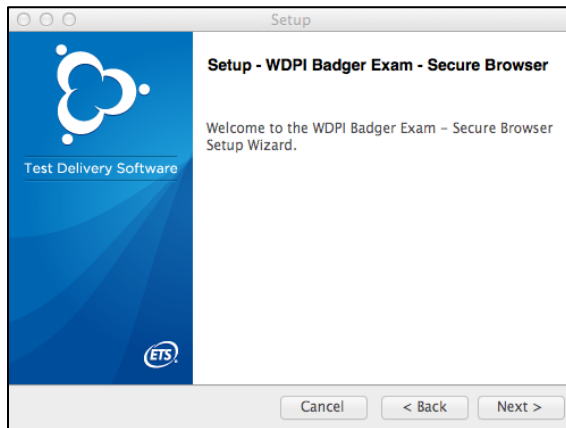
3. Select the securebrowser.dmg icon located on the desktop or downloads folder.



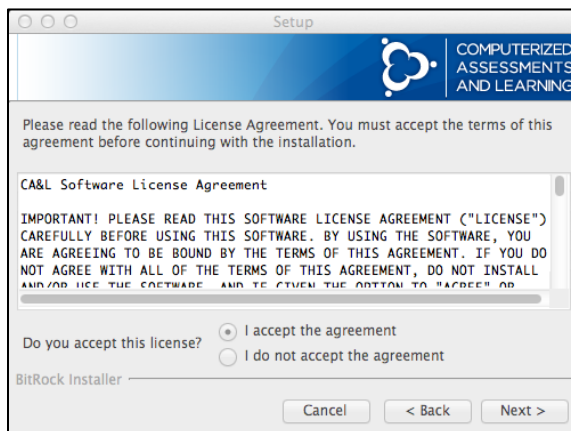
4. Select the SecureBrowser icon in the popup window.



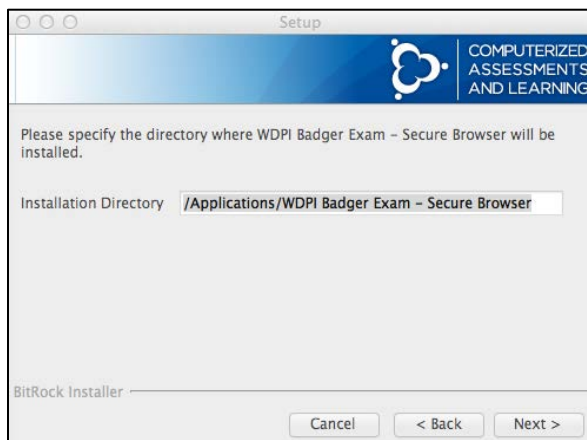
5. A popup will present the following statement: “SecureBrowser” is an application downloaded from the Internet. Are you sure you want to open it?” Click **Open**.
6. Another popup will ask for your password. Be sure you have admin rights to the computer. Enter your password and click **OK**.
7. Follow the on screen installation directions to allow the software to install.



8. Accept the licensing agreement and click **Next**.



9. Specify where the Secure Browser should be installed, and click **Next**.



10. When the installation completes, the Secure Browser can be launched by double-clicking the Secure Browser icon on your desktop or go to:
Applications → WDPI Badger Exam – Secure Browser → **dB**T



Disabling Spaces in Mission Control on Mac 10.7–10.10 computers

Follow the instructions below to disable Spaces. Spaces should be disabled on computers that students will be using.

1. Navigate to Apple → System Preferences
2. In System Preferences, click the [Keyboard] icon. The Keyboard window will be displayed.
3. Click the [Keyboard Shortcuts] tab. The Keyboard Shortcuts options will be displayed.



NOTE: Mac 10.9 uses the label [Shortcuts].

4. In the left panel, click “Mission Control.” The right panel will show all Mission Control options.
5. In the right panel, make sure the boxes for the following are NOT checked:
 - ☐ Move left a space
 - ☐ Move right a space
 - ☐ Switch to Desktop 1 (this may already be unchecked.)
6. To re-enable Spaces, follow steps 1–4 again, and check the boxes for spaces.

Uninstalling the previous Mac OS X Secure Browser

If you need to uninstall the Secure Browser for any reason, follow these instructions.

1. Go to: Applications → WDPI Badger Exam – Secure Browser → **uninstall**
2. Follow the on screen directions to allow the software to uninstall.
3. When complete, click **OK**.

Network Installation Information for Mac OS X (Network Administrators)

The appropriate Secure Browser must be installed on each computer that will be used for online testing. While we strongly recommend that you install the Secure Browser on each individual computer that will be used, you can also push the browser out to all computers through a network by copying browser files from the network to individual computers or through third-party installation programs.

This document provides network installation instructions for computers using the following supported Mac OS X operating systems: 10.7, 10.8, 10.9, 10.10, and the Apple Remote Desktop application.

Installing the Mac OS X Secure Browser Using Apple Remote Desktop

1. Log into an administrator computer on your network. This computer should have Apple Remote Desktop installed and running.
2. Download the correct Mac OS X browser from the portal.
3. Click the downloaded icon to unzip and save the .dmg file onto your administrator computer.
4. Open the .dmg file and select the .app file.
5. Open Apple Remote Desktop.
6. In the Apple Remote Desktop window, select a Computer List.
7. Select one or more computers from the Computer List onto which you would like to install the Secure Browser.
8. Select Manage > Copy Items.
9. Select the browser .app file (from Step 4).
10. Select copy options, including your preferred destination on the target machine.
11. Click [Copy].

Closing the Mac Secure Browser

In the event that there is a need to force an exit of the Secure Browser before completion of a test, enter **Shift + Esc + E**.

Assistive Technology, Badger 3-8, Secure Browser

Students requiring external assistive devices will need to have a different Secure Browser installed. The District and School Technology Coordinators are responsible for installing the correct browsers on the devices used for testing at a school. Students using use braille devices (Jaws and Voice-Over), speech-to-text, or other assistive technology or software must have “Permissive Mode” enabled in their settings in the Test Operations Management System (TOMS). Permissive Mode is a setting that allows assistive software and devices to function with the Assistive Technology WDPI Badger Exam Secure Browser. For more on setting Permissive Mode in TOMS, see the Section 5 of the TOMS User/Student Management Manual.

On the [TOMS Dashboard](#) and on the [DPI website](#) (both available to access through the DPI website or by linking directly) users will see options to download Secure Browsers to each device used for testing. Select the browser named “**Assistive Tech WDPI Badger Exam 3-8, Secure Browser**” to download it to the device. After the start of test administration, browsers will only be

able to be installed by logging into TOMS. Follow the steps outlined in this section for each device.

Students requiring any external assistive technology devices can only test with computers using Windows or Mac OS X operating systems. The Assistive Technology Secure Browser cannot be downloaded to Chromebooks or tablets.

Users can install both the Badger Exam 3-8 Secure Browser and the Assistive Technology, Badger Exam 3-8, Secure Browser on the same device. If a student who requires accessibility resources attempts to take the Badger Exam on a computer with only the standard Secure Browser installed, the browser will block the use of additional assistive technology.

Assistive Tech WDPI Badger Exam Secure Browser Windows EXE V: 2.7.0

Use this version to install the secure browser on individual computers for Students using braille or other assistive technology and software.

 **Download**

Assistive Tech WDPI Badger Exam Secure Browser Windows MSI V: 2.7.0

Use this version to install the secure browser on multiple computers for Students using braille or other assistive technology and software.

 **Download**

iOS (iPad) Secure Browser

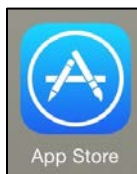
The Secure Browser for online testing for iPads can be downloaded from the App store. The process for installing the Secure Browser is the same as for any other application.

The iPad Secure Browser is supported on iPads 2 and newer running iOS 6.0–8.0. (The iPad Mini is not supported.) The Guided Access feature must also be enabled.

Downloading and Installing the iOS Secure Browser

The Secure Browser for online testing for iPads can be downloaded from the App store. The process for installing the Secure Browser is the same as for any other application.

1. On each testing iPad, confirm that the iPad's date, time, and time zone are set to the correct date, time, and time zone of the test center location.
2. Open a browser and go to the DPI Badger Portal at <https://wdpibadger.caltesting.org> and select the **WDPI Badger Exam Secure Browsers for iPad** or open the App Store. The process for installing the Secure Browser from the App Store is the same as for any other application.



3. Search the App Store for “WDPI”.
4. Select the **WDPI Badger Exam – Secure Browser** app.

5. Tap **GET** to download the **WDPI Badger Exam – Secure Browser** app.



NOTE: This step may include an update → tap **Update**.

6. The **WDPI Badger Exam – Secure Browser** app will download to the iPad Home screen.

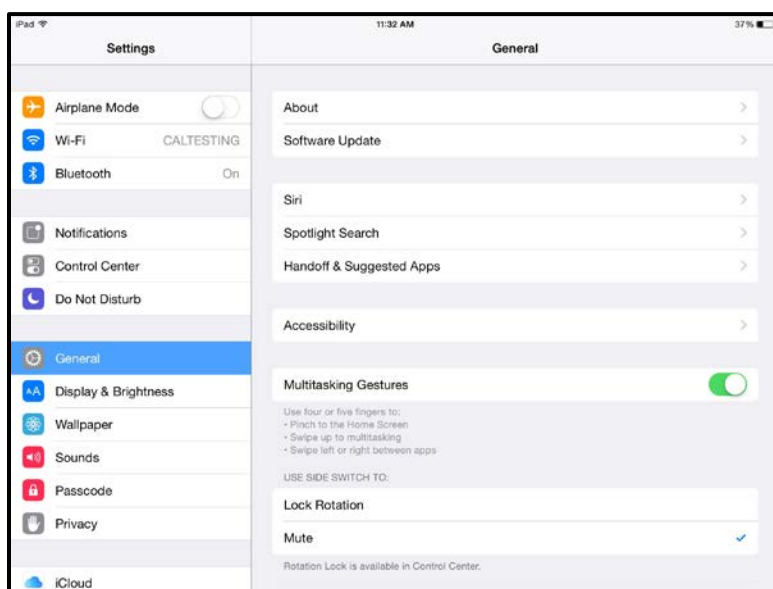


Enabling Guided Access

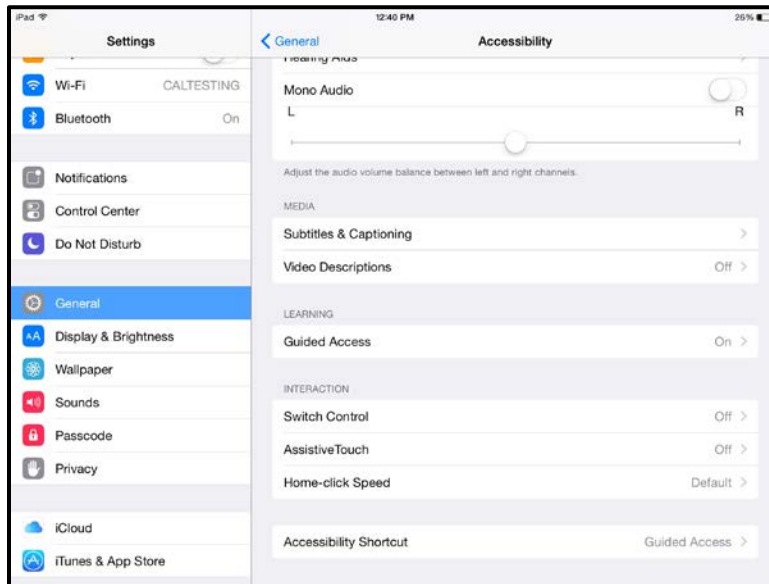


NOTE: Display of settings may vary slightly based on iOS version. The following images are based on iOS 8.1.2.

1. Under Settings, tap **General**.
2. Tap **Accessibility**.

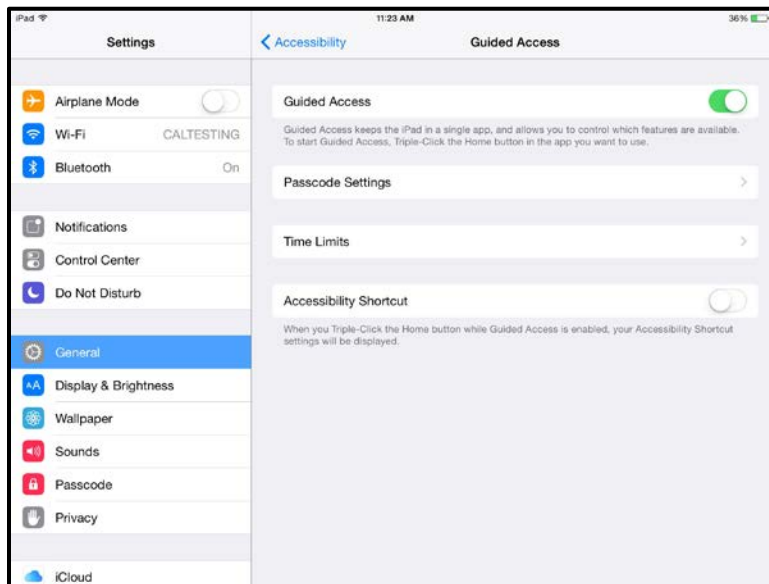


3. Tap **Guided Access**.

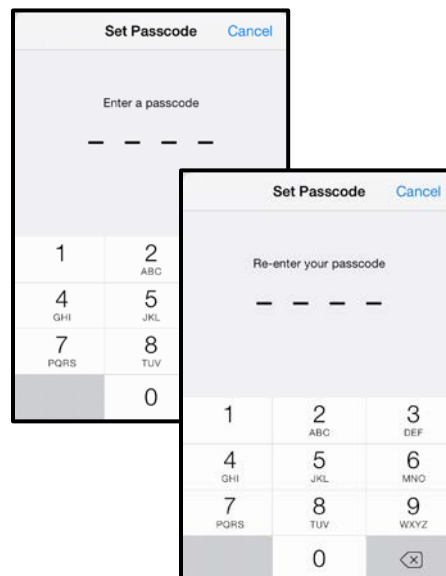
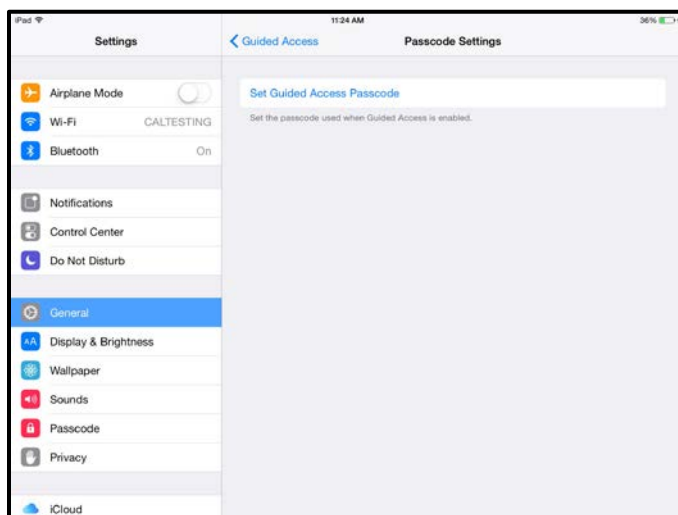


4. Toggle the Guided Access to the **ON** position.

5. Tap **Passcode Settings**.



6. Tap **Set Guided Access Passcode**.
7. Enter a four digit passcode.
8. Re-enter the four digit passcode.



WARNING: Do not forget the passcode. The passcode is needed for exiting the **WDPI Badger Exam – Secure Browser** app, and prevents the iPad test taker from using other apps during testing. The test taker should NOT be given the passcode.

Activating Guided Access Before a Test Session Begins

Before using the Secure Browser for a Practice Test or for taking the Badger Exam, Guided Access must be engaged.

1. Tap the **WDPI Badger Exam – Secure Browser** app.



2. As the app launches, triple click the **Home** button to initiate Guided Access.
3. A pop-up message will appear saying Guided Access has started.



NOTE: When Guided Access is activated, students cannot switch to any other applications or take screenshots.

Deactivating Guided Access After a Test Session Ends

1. Triple-click (press) the Home button.
2. Enter your Guided Access passcode. This must be the same passcode that you selected when you enabled Guided Access.



Listening. Learning. Leading.®



3. Tap the [End] button in the upper left corner. A pop-up message will appear saying Guided Access has ended.

Closing the iPad Secure Browser (iOS 6.0–6.1)

1. Double-click (press) the Home button at the bottom of the iPad. This will open the multitasking bar.
2. Press the minus sign on the **WDPI Badger Exam – Secure Browser** app icon until it disappears.

Closing the iPad Secure Browser (iOS 7.0–8.1.2)

1. Double-click (press) the Home button. This will open the multitasking screen.
2. Locate the **WDPI Badger Exam – Secure Browser** app preview and slide it upward.

Section 4: Braille Hardware and Software

Braille Hardware

The following devices are to be used for students accessing tests with a braille accommodation.

For students: A refreshable braille display. We recommend that the display have a minimum of 40 cells.

For Test Administrators: ViewPlus Tiger Max Embosser



Reminder: All printed test materials for secure tests must be shredded immediately after a test session ends.

Braille Software

Requirements for Test Administrator Computers

Test Administrators (TAs) administering tests to students who require braille must have the following software installed on their machine prior to testing. The software is necessary to process these students' print requests.

ViewPlusTiger Max Embosser and the supporting **ViewPlus Desktop Embosser driver**

- The Desktop Embosser Driver can be downloaded from <http://downloads.viewplus.com/drivers/desktop-braille-embosser/>.
- The download includes the Tiger Viewer software, which is needed to handle print requests for items and passages that contain tactile or spatial components.



NOTE: Braille embossers require special braille paper. Using higher quality paper will reduce the paper dust left in the embosser, and therefore reduce the likelihood of mechanical failure.

Requirements for Student Computers

The Test Delivery Engine currently supports the braille interface on Windows 7 and Windows 8.1 machines only.

Windows Assistive Tech WDPI Badger Exam Secure Browser must be installed on all machines used for student testing, including tests administered using the Braille interface.

JAWS Screen Reader (version 12, 13, 14, 15 or 16)

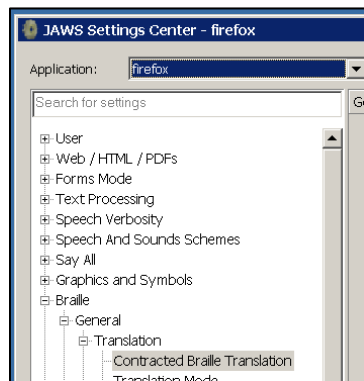
Refreshable braille display that is compatible with Windows 7 and the version of JAWS that is on the computer. We recommend that the braille display have a minimum of 40 cells.

For more information about JAWS, including product download and purchase, go to <http://www.freedomscientific.com/products/fs/jaws-product-page.asp>.

Applying Settings for Contracted/Uncontracted Braille

In order for students to use Contracted or Uncontracted Literary Braille, the correct JAWS setting must be applied prior to launching the Secure Browser.

1. Open the JAWS Settings Center. The Settings Center is accessible via the JAWS Menu > Utilities.
2. Select Firefox from the “Application” drop-down menu.
3. From the panel on the left side of the window, go to the following option (as pictured): Braille > General > Translation > Contracted Braille Translation.



4. For Uncontracted Braille, set the value to “Off.” For Contracted Braille, set the value to “Input and Output.” Additionally, ensure that the following three settings are checked (and only these settings are checked):
 - Active cursor follows Braille display
 - Enable Braille Auto Detection
 - Enable Word Wrap
5. Click [Apply] and then click [OK].

In addition, the following optional JAWS settings may be adjusted for individual students based on student needs prior to administering their assessments.

- Adjust JAWS voice profile (Optional)
- Adjust JAWS speaking speed (Optional)
- Adjust JAWS punctuation (Optional)

If adjusting these optional settings for a student, the steps described for each option must be taken prior to launching the Secure Browser.





Adjusting JAWS Voice Profile

The JAWS voice profile refers to the voice used by JAWS. Users can adjust the JAWS voice profile by following the instructions below.

1. Go to JAWS Menu > Options.
2. Select Voices Adjustment.
3. In the Profile section, select a Voice Profile from the Name drop-down menu.
4. Click [OK].

Adjusting JAWS Speaking Rate

Users can adjust the rate of speed that JAWS speaks by following the instructions below.

1. Go to JAWS Menu > Options.
2. Select Voices Adjustment.
3. In the Voice section, adjust the “Rate” using the slide-bar.
4. Click [OK].

Adjusting JAWS Punctuation

The default JAWS punctuation setting for which the braille Interface has been optimized is “Most.” This means that JAWS will read most punctuation that appears on the screen. However, users may adjust the JAWS punctuation based on an individual student’s needs and preferences by following the instructions below.

1. Go to JAWS Menu > Options.
2. Select Voices Adjustment.
3. In the Voice section, select a punctuation setting from the Punctuation drop-down menu. The options include “None,” “Some,” “Most,” and “All.”
4. Click [OK].

Section 5: Text-to-Speech

Secure Browser

The Secure Browsers are configured to recognize several known voice packs to provide the text-to-speech accommodation. The Secure Browsers detect pre-installed voice packs on the students' machines. When a student who is using text-to-speech logs into a test session and has been approved for testing, the Secure Browser will look for voice packs on the student's machine. When it recognizes an approved voice pack, the one with the highest priority rating will be used.

If any of the approved voice packs has also been set as the default voice on the computer, then that voice pack will always get the highest priority.

Note: The Secure Browser will select voices that enable control of the speech rate, even if a non-default voice gets selected.

Voice packs on Chromebooks

If additional voice packs have been downloaded to a Chromebook, the Secure Browser will only recognize the Chromebook's default voice pack.

Configuring Text-to-Speech Settings

This section provides information on ensuring that text-to-speech for online testing will work appropriately on computers running Windows XP (Service Pack 3), Vista, 7, 8.0, or 8.1.

The speech feature on Windows operating systems is user interface (UI) driven. This means that the text-to-speech preferences used to administer the text-to-speech accommodation are located within the computer's system preferences. Follow the steps below to configure text-to-speech preferences.

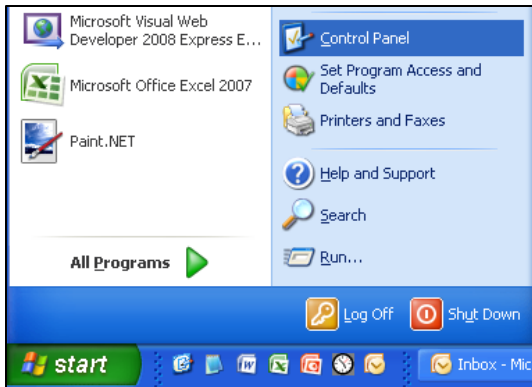
As a reminder, text-to-speech is available only when the Secure Browser is used. Students can access the Practice and Training Tests using the Secure Browser.

Windows XP

The instructions in this section are for computers running Microsoft Windows XP.

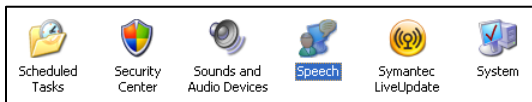
Step 1: Access Control Panel

Click the [Start] button and then click the Control Panel link.



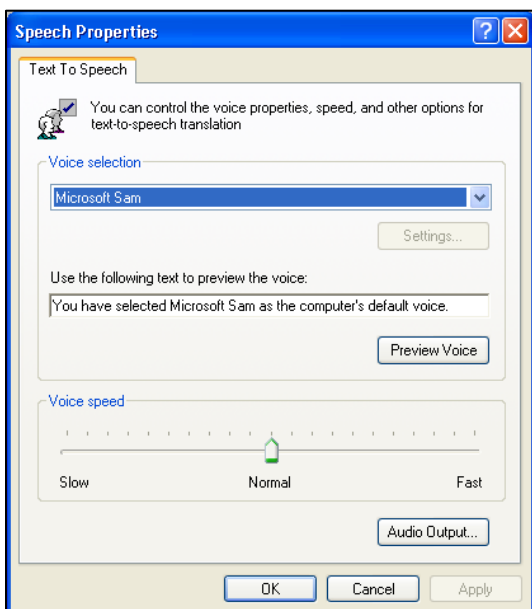
Step 2: Access Speech Options

In the Control Panel window, click the [Speech] icon. This will bring up the Speech properties window.



Step 3: Set Speech Preferences

1. Select your desired Voice Selection from the drop-down menu. (You may have only one voice available.)
2. Click [Preview Voice] to verify that you can hear the voice.
3. Set the desired Voice speed. Click [Audio Output] to listen to the settings. You can adjust the settings as desired.
4. When you are done, click [OK] to save your settings, and then click the Red [X] at the top right of the screen to close the window.



Windows 7

The instructions in this section are for computers running Microsoft Windows 7

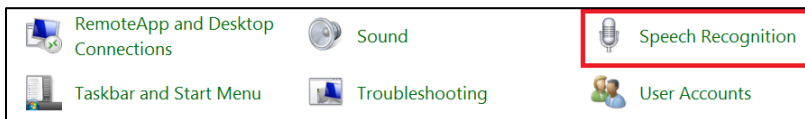
Step 1: Access Control Panel

Click the [Start] button and then click the Control Panel link.



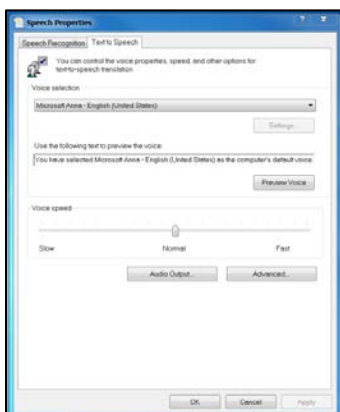
Step 2: Access Speech Options

In the Control Panel window, click the [Speech Recognition] icon. This will bring up the Speech properties window.



Step 3: Set Text to Speech Preferences

1. Click [Text to Speech] from the left column
2. Select your desired Voice Selection from the drop-down menu. (You may have only one voice available.)
3. Click [Preview Voice] to verify that you can hear the voice.
4. Set the desired Voice speed. Click [Audio Output] to listen to the settings. You can adjust the settings as desired.
5. When you are done, click [OK] to save your settings, and then click the Red [X] at the top right of the screen to close the window.

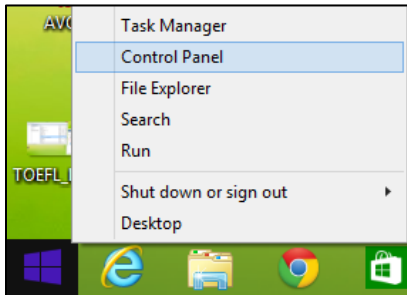


Windows 8.1

The instructions in this section are for computers running Microsoft Windows 8.1

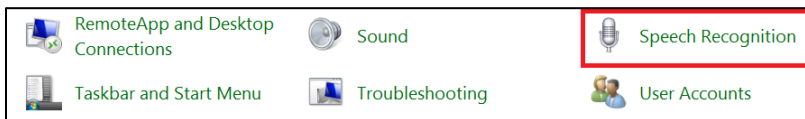
Step 1: Access Control Panel

Right click the [Start] button and then click the Control Panel link.



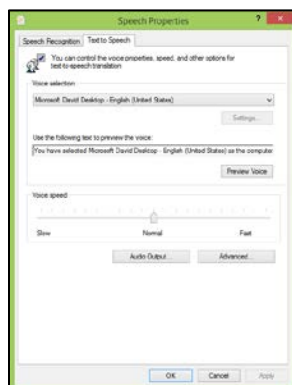
Step 2: Access Speech Options

In the Control Panel window, click the [Speech Recognition] icon. This will bring up the Speech properties window.



Step 3: Set Speech Preferences

1. Click [Text to Speech] from the left column.
2. Select your desired Voice Selection from the drop-down menu. (You may have only one voice available.)
3. Click [Preview Voice] to verify that you can hear the voice.
4. Set the desired Voice speed. Click [Audio Output] to listen to the settings. You can adjust the settings as desired.
5. When you are done, click [OK] to save your settings, and then click the Red [X] at the top right of the screen to close the window.



Section 6: User Support

For further information please use one of the following:

<http://oea.dpi.wi.gov/assessment/Smarter>

Badger Exam Help Desk

- Phone: 1-844-711-6493
- Email: badgerexamhelpdesk@ets.org

Help Desk Hours:

- Monday through Friday
- 7:00 a.m. to 5:00 p.m. Central Time

Section 7: Local Caching Software

LCS information will be ready the week of March 16th. Look for an updated TCM at that time.



Listening. Learning. Leading.®



Appendix A: IP Addresses and URLs for Badger Exam Systems

IP Addresses and URLs for Badger Exam Systems

Site	URL	IP Addresses
Portal	wdpibadger.caltesting.org	72.4.115.187
Test Delivery	wdpibadger-tss.caltesting.org	72.4.115.186
TOMS	wdpibadger-toms.caltesting.org	72.4.115.185

Appendix B – School Technology Coordinator Checklist

Technology Readiness Checklist			
✓	Action Item	Preparation Timeline	Information Resource
<input type="checkbox"/>	Step 1 Verify that your school's network meets the requirements, is configured for testing, and can connect to the Internet. Conduct network diagnostics to confirm sufficient bandwidth.	Can begin immediately.	Network Requirements Document
<input type="checkbox"/>	Step 2 Verify that all of your school's computers that will be used for online testing meet the minimum hardware and software requirements.	Can begin immediately.	System Requirements Document
<input type="checkbox"/>	Step 3 Install the Secure Browser on your testing devices (install the Assistive Technology Secure Browser if there are students that will require assistive technology).	3 to 4 weeks before testing begins in your school.	Technology Coordinators Manual, Section 3
<input type="checkbox"/>	Step 4 Determine if an LCS would be beneficial for testing. Install a WDPI Badger – LCS and configure testing computers to connect to the LCS.	3 to 4 weeks before testing begins in your school.	Technology Coordinators Manual, Section 7
<input type="checkbox"/>	Step 5 Take a practice test from each testing device (using a student network and/or device login as necessary).	3 to 4 weeks before testing begins in your school.	DPI Website
<input type="checkbox"/>	Step 6 For Windows computers disable Fast User Switching.	2 to 3 weeks before testing begins in your school.	Technology Coordinators Manual, Section 3
<input type="checkbox"/>	Step 7 For Mac OS 10.7 to 10.10 computers disable Spaces in Mission Control.	2 to 3 weeks before testing begins in your school.	Technology Coordinators Manual, Section 3
<input type="checkbox"/>	Step 8 Confirm that your braille hardware is functioning and configured for the testing device to which it is connected. Check for other accommodation software that may be needed.	2 to 3 weeks before testing begins in your school.	Technology Coordinators Manual, Section 4
<input type="checkbox"/>	Step 9 Ensure that all forbidden applications except those identified as necessary by the District Technology Coordinator are uninstalled from testing computers.	1 to 2 weeks before testing begins in your school.	
<input type="checkbox"/>	Step 10 During the testing window, ensure availability to follow up internally on any technical issues that may arise.	Ongoing throughout the testing window.	



Listening. Learning. Leading.®



Document Change History

Revision Date	Summary of Changes
2/13/15	Added Windows network deployment.
3/10/2015	Added Mac OS X and iPad installation instructions